
Ukázky aplikací matematiky

Jiří Tůma

2015

<http://www.karlin.mff.cuni.cz/~tuma/aplikace15.htm>

tuma@karlin.mff.cuni.cz

Kapitola 1

Úvod do šifrování

Základní pojmy - obsah

- *Základní pojmy*
 - Ceasarova šifra
 - Posuvná šifra
 - Útok hrubou silou

Historie šifrování

- historie šifrování je několik tisíc let stará
- *šifrování* skrývá obsah zprávy
- neskrývá samotnou zprávu

Ceasarova šifra

KOSTKY JSOU VRZENY

Posuvná šifra

je to Caesarova šifra s variabilní délkou posunutí
k šifrování potřebujeme znát nejen *otevřený text*
ale také *klíč*

například pro klíč $k = 5$ – posunutí o 5

KOSTKY JSOU VRZENY

Nevýhoda posuvné šifry

malý prostor klíčů – dají se všechny vyzkoušet

říká se tomu *útok hrubou silou*

OXGB OBWB OBVB

Jednoduchá záměna - obsah

- *Jednoduchá záměna*
 - Popis šifry
 - Slabiny jednoduché záměny

Jednoduchá záměna

Cesarova šifra nahrazuje každé písmeno otevřeného textu písmenem, které je pod ním v následující tabulce

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

podobně posuvnou šifru s posunutím $k = 9$ zapíšeme tabulkou

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

jako druhý řádek můžeme použít libovolnou permutaci 26 písmen abecedy

taková šifra se nazývá *jednoduchá záměna* nebo *jednoduchá substitute* nebo *simple substitution*

Klíč pro jednoduchou záměnu

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

zašifrujeme zprávu

VEZEME PENICILIN

základní slabina jednoduché záměny

Úprava textu před zašifrováním

vynecháme mezery

VEZEMEPENICILIN

nebo nahradíme mezery málo používaným písmenem – třeba X

VEZEMEXPENICILIN

proč to nepomůže ?

Frekvenční analýza

hrubá síla nepomůže

Fekvenční analýza

hrubá síla nepomůže – klíčů je

frekvence jednotlivých písmen v přirozeném jazyce pomůžou

v klasických dobách kryptoanalytici používali

-
-
-
-

dnes existují jednoduché algoritmy, které

- spolehlivě najdou 70% textu
- najdou šifrové podoby samohlásek

Jednoduchá transpozice - obsah

- *Jednoduchá transpozice*
 - Popis transpoziční šifry
 - Kódová kniha

Jednoduchá transpozice

založená na přeházení písmen v otevřeném textu

prostor klíčů pro zprávy délky 200 je 200!

proto se používal postup založený na klíči - SLIZOUN

zašifrujeme DNES VECER VYBOUCHNE NA RECEPCI

Dvojitá transpozice

dva klíče: první SLIZOUN, druhý VYMEKNE

před zprávou musela být vždy uvedena její délka

základní bezpečnostní opatření – neposílat dvě zprávy stejné délky zašifrované stejnými klíči

Kódová kniha

jednotlivá slova se nahrazují skupinami 5 čísel nebo písmen

jde vlastně o slovník

MINISTR FINANCI – 00007, BURES

PRESIDENT – 00001, HLAVA

A – 98765, RANDE

HRAD – 13856, BEDQR

NA – 85479, TWHPU

VECERE – 36820, SALAM

DNES – 70333, AGENT

HLAVA RANDE BURES SALAM TWHPU AGENT

00001 98765 00007 36820 85479 13856

Vigenérova šifra - obsah

- *Vigenérova šifra*
Popis

„Nerozlužitelná šifra“

používá periodicky několik různých posunutí abecedy

délka posunutí se opět udávala heslem

SLIZOUN pomocí tabulky

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

dával posunutí 18 11 8 5 14 20 13

SLIZOUNSLIZOUN

KOCKALEZEDIROU

Historie

šifru popsal již v roce 1586 Blaise de Vigenére

rozluštil ji až Charles Babbage (1791-1875), profesor matematiky na Cambridge University

algoritmus vymyslel William F. Friedman (1891-1961) kolem roku 1920

založený na *indexu koincidence*

jeden z nejdůležitějších pojmů v kryptologii

využívá slabinu

Index koimcidence - obsah

- *Index koimcidence*
Definice

Index koincidence

je definován pro dva texty

protezyrukoujsoucimdalcitlivejsiaobratnejsinejenze
francouzskyreziseroscarovychdeljeanjacquesannaudtv

bezrukypacientumumoznujivratitsedobeznehozivotaal
urcesedmiletvtibetucijmenaruzeprevezmenafebiofestu

index koincidence dvou textů je procento míst, kde jsou stejná
písmena

dvě náhodně generované posloupnosti písmen by měly index
koincidence rovný

Očekávaná hodnota indexu koincidence

označíme-li pravděpodobnosti výskytu písmen v jazyce

$p_0, p_1, p_2, \dots, p_{25}$

bude očekávaná hodnota indexu koincidence tohoto jazyka

očekávané hodnoty indexu koincidence pro různé jazyky

Slabina periodického hesla

stejně dvojice po sobě jdoucích písmen v otevřeném textu

xy ve vzdálenosti násobku délky klíče

je zašifrována stejnou dvojicí písmen xy

na tomto pozorování je založený *Kasiského test*

Friedrich Kasiski (1805-1881)

v šifrovém textu hledáme opakované výskyty stejných dvojic

některé vznikly náhodně, jiné jako výše, těch je víc

spočteme vzdálenosti stejných dvojic

najdeme číslo, které dělí většinu vzdáleností

to je odhad délky klíče, zbytek je snadný

Polyalfabetická šifra - obsah

- *Polyalfabetická šifra*
Popis

Polyalfabetická šifra

podobná Vigenérově, pouze místo různých posunutí na různých místech používá obecné permutace

```
abcdefghijklmnopqrstu  
vwxyz  
gkqwhrjvoisnazcub  
dxplfytme  
cintzuhSYMjABvoel  
xwpkfqgrd  
ekrwxpavqbslcfi  
tudgjmhnyzo  
dqcuimhvrelnwg  
ofjkztysabpx
```

permutace periodicky opakujeme

```
1234123412  
BECHEROVKA
```

Generování klíče

klíčem pro polyalfabetickou šifru je posloupnost permutací

jak ji generovat

jak si ji pamatovat, jak ji předávat

před téměř 100 lety začaly vznikat „šifrovací stroje“

nejznámější jsou Enigma, Hagelin

Polyalfabetická šifra a index koincidence

Algoritmus pro luštění Vigenérový šifry

založený na indexu koincidence

zachycený šifrový text zapisujeme postupně do 2,3,4,... sloupců

je-li počet sloupců násobkem délky klíče, jsou všechna písmena v každém sloupci zašifrována stejným posunutím

v různých sloupcích různým

pokud počet sloupců není násobkem délky klíče, jsou různá různá písmena v témže sloupci výsledkem šifrování různým posunutím

Nalezení délky klíče

pro každý sloupec v dané tabulce spočteme index koincidence

pak spočteme průměr indexů koincidence přes všechny sloupce

vyjde něco jako

zbytek je snadný

Vernamova šifra

dne 13.9.1918 Gilbert Vernam požádal o americký patent na údajně zcela bezpečnou šifru

šlo vlastně o Vigenérovu šifru s náhodně generovaným klíčem téže délky jakou má otevřený text

absolutní bezpečnost Vernamovy šifry dokázal až Claude Shannon po roce 1945

intuitivně ji lze nahlédnout

Absolutní a výpočetní bezpečnost

aboslutní bezpečnost - ze šifrovaného textu nelze usoudit nic o otevřeném textu, jakýkoliv možný otevřený text je stejně pravděpodobný i ve chvíli, kdy známe šifrovaný text

Shannonova klec

moderní šifry se snaží imitovat Vernamovu šifru

z krátkého klíče, třeba 128 bitů generují nějakým algoritmem *proud klíče*, který vypadá náhodně

výpočetní bezpečnost - nic neusoudíme ani za použití všech dostupných výpočetních prostředků